PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Original) A method of generating a key stream comprising:

applying a cryptographic function on input values selected from a first array of values to generate output values;

selecting mask values from a second array of values; and

combining the output values with the mask values to generate a key stream block for the key stream;

wherein the first and second arrays are finite.

2. (Original) The method of claim 1, further comprising: generating the second array from the first array.

3. (Currently Amended) The method of claim 2, further comprising: using a linear feedback shift register (LFSR) to generate the first array, wherein the values of the first array correspond to the values of the LFSR ~~LSFR~~ states.

4. (Original) The method of claim 3, further comprising: clocking the LFSR to generate the second array.

5. (Original) The method of claim 3, wherein each value comprises of one or more words, each of two or more bytes and wherein using the LFSR to generate the first array comprises:

copying words of a key and words of an initialization vector into the LFSR;

performing a byte-wise substitution on at least one byte of a word in the LFSR to generate a corresponding replacement word in the LFSR;

mixing at least two bytes of a replacement word in the LFSR; and

mixing at least two words in the LFSR to generate the first array.

6. (Original) The method of claim 1, further comprising:

applying the cryptographic function on updated input values selected from an updated first array of values to generate updated output values;

selecting updated mask values from an updated second array of values; and

combining the updated output values with the updated mask values to generate a new key stream block for the key stream.

7. (Currently Amended) The method of claim 6, further comprising: setting the values of the first array as the values of first linear feedback shift register (LFSR) states; and clocking the LFSR ~~LSFR~~ to generate the updated first array.

8. (Currently Amended) The method of claim 6, further comprising: setting the values of the second array as the values of second LFSR states; and clocking the LFSR ~~LSFR~~ to generate the updated second array.

9. (Original) The method of claim 1, wherein the number of input values and the number of output values are equal.

10. (Original) The method of claim 1, wherein the first and second array each comprises seventeen values.

11. (Original) The method of claim 1, wherein each value comprises of one or more words and wherein each word comprises two or more bytes.

12. (Original) The method of claim 11, wherein applying the cryptographic function comprises:

performing a byte-wise substitution of at least one byte of an input value to generate primary intermediate values; and

mixing at least two bytes of a primary intermediate value to generate a secondary intermediate value to generate the output values.

13. (Original) The method of claim 12, wherein performing the byte-wise substitution of at least one byte comprises: performing a nonlinear substitution of the at least one byte.

14. (Original) The method of claim 13, wherein performing the nonlinear substitution of the at least one byte comprises: performing a key-dependent Sbox substitution on the at least one byte.

15. (Original) The method of claim 14, wherein performing the key-dependent Sbox substitution of the at least one byte comprises:

combining a first key byte with the at least one byte to generate a first combined byte; and

substituting the first combined byte with a byte value from a pre-determined array.

16. (Original) The method of claim 15, further comprising: generating the first key byte based on a secret key of one or more words.

17. (Original) The method of claim 16, wherein generating the first key comprises:

performing a byte-wise substitution of at least one byte of a word of the secret key to generate a corresponding replacement word; and

mixing at least two bytes of a replacement word to generate the first key byte.

18. (Original) The method of claim 15, wherein performing the key dependent Sbox substitution further comprises:

combining a second key byte with the substituted first combined byte to generate a second combined byte; and

substituting the second combined byte with a byte value from the predetermined array.

19. (Original) The method of claim 12, wherein mixing at least two bytes of the primary intermediate values comprises: mixing at least two bytes using a minimum distance separable matrix multiplication.

20. (Original) The method of claim 19, wherein the minimum distance separable matrix multiplication comprises operations over a Galois Field comprising 256 elements.

21. (Original) The method of claim 12, wherein applying the cryptographic function further comprises: mixing at least two input values to generate the primary intermediate values.

22. (Original) The method of claim 21, wherein mixing at least two input values comprises: mixing at least two input values based on modular arithmetic.

23. (Original) The method of claim 22, wherein mixing at least two input values comprises:

adding the input values to generate a mixed value, wherein the mixed value is a primary intermediate value corresponding to a first input value; and

adding the mixed value with a second input value to generate a primary intermediate value corresponding to the second input value.

24. (Original) The method of claim 12, wherein applying the cryptographic function further comprises: mixing at least two secondary intermediate values to generate the output values.

25. (Original) The method of claim 24, wherein mixing at least two secondary intermediate values comprises: mixing at least two input secondary intermediate values based on modular arithmetic.

26. (Original) The method of claim 25, wherein mixing at least two secondary intermediate values comprises:

adding the secondary intermediate values to generate a mixed value, wherein the mixed value is an output value corresponding to a first secondary intermediate value; and

adding the mixed value with a second secondary intermediate value to generate an output value corresponding to the second secondary intermediate value.

27. (Original) Apparatus for generating a key stream comprising:

means for applying a cryptographic function on input values selected from a first array of values to generate output values;

means for selecting mask values from a second array of values; and

means for combining the output values with the mask values to generate a key stream block for the key stream; wherein the first and second arrays are finite.

28. (Original) The apparatus of claim 27, further comprising: means for generating the second array from the first array.

29. (Original) The apparatus of claim 27, further comprising:

means for applying the cryptographic function on updated input values selected from an updated first array of values to generate updated output values;

means for selecting updated mask values from an updated second array of values; and

means for combining the updated output values with the updated mask values to generate a new key stream block for the key stream.

30. (Original) The apparatus of claim 27, wherein the number of input values and the number of output values are equal.

31. (Original) The apparatus of claim 27, wherein each value comprises of one or more words and wherein each word comprises two or more bytes.

32. (Original) The apparatus of claim 31, wherein the means for applying the cryptographic function comprises:

means for performing byte-wise substitution of at least one byte of an input value to generate primary intermediate values; and

means for mixing at least two bytes of a primary intermediate value to generate a secondary intermediate value to generate the output values.

33. (Original) The apparatus of claim 32, wherein the means for performing byte-wise substitution comprises: means for performing a key-dependent Sbox substitution on the at least one byte.

34. (Original) The apparatus of claim 32, wherein the means for mixing at least two bytes of the primary intermediate values comprises: means for mixing at least two bytes using a minimum distance separable matrix multiplication.

35. (Original) The apparatus of claim 32, wherein the means for applying the cryptographic function further comprises: means for mixing at least two input values based on modular arithmetic to generate the primary intermediate values.

36. (Original) The apparatus of claim 32, wherein the means for applying the cryptographic function further comprises:

means for mixing at least two secondary intermediate values based on modular arithmetic to generate the output values.

37. (Previously Presented) A machine readable medium having one or more instructions for generating a key stream, which when executed by a machine, causes the machine to perform operations comprising:

applying a cryptographic function on input values selected from a first array of values to generate output values;

selecting mask values from a second array of values; and

combining the output values with the mask values to generate a key stream block for the key stream;

wherein the first and second arrays are finite.

38. (Previously Presented) The medium of claim 37, further comprising one or more instructions to cause the machine to perform operations comprising: generating the second array from the first array.

39. (Previously Presented) The medium of claim 37, wherein each value comprises of one or more words and wherein each word comprises two or more bytes and wherein applying the cryptographic function comprises one or more instructions to cause the machine to perform operations comprising:

performing a byte-wise substitution of at least one byte of an input value to generate primary intermediate values; and

mixing at least two bytes of a primary intermediate value to generate a secondary intermediate value to generate the output values.

40. (Previously Presented) The medium of claim 39, wherein performing the byte-wise substitution comprises: comprises one or more instructions to cause the machine to perform operations comprising: performing a key-dependent Sbox substitution on the at least one byte.

41. (Previously Presented) The medium of claim 39, wherein mixing at least two bytes of the primary intermediate values comprises one or more instructions to cause the machine to perform operations comprising: mixing at least two bytes using a minimum distance separable matrix multiplication.

42. (Previously Presented) The medium of claim 41, wherein applying the cryptographic function further comprises one or more instructions to cause the machine to perform operations comprising: mixing at least two input values based on modular arithmetic to generate the primary intermediate values.

43. (Previously Presented) The medium of claim 41, wherein applying the cryptographic function further comprises one or more instructions to cause the machine to perform operations comprising: mixing at least two secondary intermediate values based on modular arithmetic to generate the output values.

44. (Original) Apparatus for generating a key stream comprising:

a linear feedback shift register (LFSR) configured to generate a first array of values, wherein the values of the first array corresponds to the values of the LFSR states;

a nonlinear filter module configured to apply a cryptographic function on input values selected from the first array to generate output values; and

a combining module configured to combine the output values with mask values selected from a second array of values to generate a key stream block for the key stream; wherein the first and second arrays are finite.

45. (Original) The apparatus of claim 44, wherein the LFSR is configured to generate the second array from the first array.

46. (Original) The apparatus of claim 44, wherein the number of input values and the number of output values are equal.

47. (Original) The apparatus of claim 44, wherein the first and second array each comprises seventeen values.

48. (Original) The apparatus of claim 44, wherein each value comprises of one or more words and wherein each word comprises two or more bytes.

49. (Original) The apparatus of claim 48, wherein the nonlinear filter module comprises:

a byte substitution module configured to perform byte wise substitution of at least one byte of an input value to generate primary intermediate values; and

a byte mixing module configured to mix at least two bytes of a primary intermediate value to generate a secondary intermediate value to generate the output values.

50. (Original) The apparatus of claim 49, wherein the byte substitution module is configured to perform a key-dependent Sbox substitution on the at least one byte.

51. (Original) The apparatus of claim 49, wherein the byte mixing module is configured to mix at least two bytes using a minimum distance separable matrix multiplication.

52. (Original) The apparatus of claim 49, wherein the nonlinear filter further comprises: a word mixing module configured to mix at least two input values based on modular arithmetic to generate the primary intermediate values.

53. (Original) The apparatus of claim 49, wherein the nonlinear filter further comprises: a word mixing module configured to mix at least two secondary intermediate values based on modular arithmetic to generate the output values.